Report for 2005RI34B: Risk Assessment Methods for Water Infrastructure Systems

Publications

- Water Resources Research Institute Reports:
  - Thomas, N., 2006, Risk Assessment Methods for Water Infrastructure Systems, Rhode Island Water Resources Center, University of Rhode Island, Kingston, RI.

Report Follows

Introduction

The latest terrorist acts perpetrated against the nation have sprouted security concerns for its varied infrastructures. Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, released on December 17, 2003, outlined the requirements for protecting the Nation’s critical infrastructure including water resource systems. Yet, the common, effective and efficient methods for assessing risk remain obscure to many decision makers. In an attempt to remedy this knowledge void in the state-of-the-practice, this report summarizes the state-of-the-art methods in assessing risk in general and for water resource infrastructures in particular. Excerpts of this report are intended for direct distribution to decision makers in water resource.

According to Jeffrey Danneels, Sandia Laboratories, in testimony to the House on Science Committee, November 14, 2001, approximately 170,000 public water systems provide water to more than 250 million Americans. Public water systems are "water systems that provide drinking water to at least 25 people or 15 service connections for at least 60 days per year." The Environmental Protection Agency (EPA) recognizes two primary types of public water systems: 1) Community Water Systems, which provide drinking water to the same people year-round. Approximately 54,000 community water systems currently serve America's homes. Of these community water systems, about 350 are large enough to serve more than 100,000 customers. 2) Non-Community Water Systems, which serve customers on less than a year round basis. More than 116,000 systems fit this category ***(EPA, 1999)***.

A clean water system has seven main functions in the process flow. Water arrives from a source, having been pumped from a well, river, etc., to a treatment plant. The treatment plant removes impurities from the water which is then channeled to a storage tank. Distribution mains carry the clean water to industry and to service lines towards homes. From industry and homes soiled water enters the sanitary sewer system. Water resource infrastructures represent key nation assets that sustain life, life’s quality, economic expansion and prosperity. Thus, they are of great value to the nation’s security.

Attacks on water resource infrastructures could disrupt the direct functioning of key business and government activities, facilities, and systems, as well as have cascading effects throughout the Nation’s economy and society. Enhanced security features should drive all new designs and retrofits for water utility systems. Risk assessments can help guide and prioritize enhancements.

This report summarizes the varied methods and tools available to the decision maker for assessing risk at water resource facilities. It further presents the advantages and disadvantages of each method and tool. Firstly, it provides working definitions of vulnerability, exposure, risk and quantitative risk assessment. It then reviews and compares conceptual frameworks and classification schemes for risk assessment methods. The exploitation of these frameworks and schemes and of the strength of the reviewed methods leads to guidelines for the selection of risk assessment methods.

Variable Definitions

Scientists in risk assessment, whether from the same or different disciplines, too often speak different languages; permitting different acceptations of the same risk terms

(Gouldby and Samuels, 2005). Numerous definitions exist for the variables of interest in a risk assessment study. These variables include: event or threat, *outcome, scenario,* exposure, vulnerability, consequences, risk. The paragraphs that follow relay in turn the acceptations of these variables utilized herein.

Event/Threat assessment considers the full spectrum of events/threats whether natural, criminal, man-made, accidental or intentional to cause harm for given facilities or locations. The likelihood of each event/threat must be established using available information. This information can be site-specific or general. Site specific data, if available in sufficient quantity and quality, is the most desirable basis for assessing events/threats. For natural events/threats, historical data concerning frequency of occurrence and consequences can be used to determine the credibility of the given event/threat. For criminal events/threats, the crime rate by crime type recorded for similar facilities provides an indication of the same. In addition, the symbolic, strategic, or intrinsic attractiveness, values of the facility as a primary or a secondary target should inform terrorist event/threat assessment.

Exposure

Causative events *and their possible outcomes* do not constitute risk unless there is an exposure to people and the environment. Exposure is mostly defined as the act of subjecting someone or something to an influencing experience. At times, it quantifies the receptors that may be influenced by the event, for example, the number of people and their demographics. Herein we shall adopt the first definition.

In quantitative risk analysis three main aspects/angles of exposure import: its controllability, its pathway and its recipients. The first aspect, controllability of the exposure, ranges from directly and indirectly controllable to the totally uncontrollable by man. Exposure of the environment to the impacts of natural events is generally uncontrollable but its consequences could be minimized by man. The second aspect, the exposure pathway, describes the potential routes to exposure by the influencing experience. It is usually expressed in terms of surface water, groundwater, inhalation or ingestion, etc. For a given outcome to specific recipients, the total magnitude of the probability of its exposure pathways (p_e) must be less than or equal to one. The totality can be less than one because the pathway may diminish the impact of the outcome. For certain exposure the probability is one and for negligible exposure it is near zero. The third consideration, the exposed recipients captures the receptors that may be influenced by the event.

Vulnerability Assessment

The National Water Resource Association (NWRA) (2002) defines a vulnerability assessment as the identification of weaknesses in security, focusing on defined threats that could compromise the ability to provide a service. The definition of vulnerability adopted here is from the National Oceanic and Atmospheric Administration (2002), the susceptibility of resources/assets to negative impacts from threat events. Hence, a vulnerability assessment accounts for the assets that could deter or defray unwanted outcomes from an event and for their susceptibility to failure.

Consequences

When event outcome entails exposure to risk recipients and to the environment, a whole set of possible consequences may occur. Consequences represent the event impacts such as economic, social or environmental damages or improvements and may be expressed quantitatively or descriptively.

Risk Assessment

The department of Homeland Security, 2004, risk assessment is where efforts in asset assessment, threat assessments, vulnerability assessments, incident response, consequence management, and consequence analysis are integrated into a coordinated framework for determining the likelihood and the expected consequences of a suite of events. This integration provides a basis for prioritizing operational and investment decisions. Whereas vulnerability assessments stress the susceptibility to threats, risk assessments stress not only the susceptibility but also the consequences.

LITERATURE REVIEW

Campbell and Stamp, 2004, of Sandia Laboratories, provide a functional classification scheme of risk assessment methods. The intent is to provide meaning by imposing a structure that identifies relationships; thereby enabling informed use of the methods so that a method chosen is optimal for a situation given. The scheme classifies methods based on level of detail, and approach. The below table, Table 1, summarizes the classes derived. Table 2 classifies known risk assessment methods into the derived scheme.

Level		Approach		
		Temporal	**Functional**	**Comparative**
3	Abstract (Expert)	Engagement	Sequence	Principles
2	Mid-Level (Collaborative)	Exercise	Assistant	Best Practice
1	Concrete (Owner)	Compliance Testing	Matrix	Audit

Table 1 Classification Matrix
Source : Campbell and Stamp, 2004

Hence, Campbell and Stamp, 2004, classify the various risk assessment methods within three different approaches (temporal, functional and comparative) at three different detail levels (abstract, mid-level and concrete) as ranked from highest to lowest. The levels hint to the scope of the application; with the higher levels indicative of larger scopes. In addition, the levels correlate with the expertise and familiarity of the risk analyst with the facility. Analyses at the lowest level require more so system familiarity than expertise and are best conducted by the facility owner. Analyses at the highest level require more expertise than familiarity and are best suited for the expert. (Expert here refers to an outside consultant who is knowledgeable in assessment methods but unfamiliar with the target system. Owner refers to someone who is not knowledgeable in assessment methods but is familiar with the target system.)

Following definitions from Campbell and Stamp, 2004, A temporal method stresses a system through the actual application of tests. These “tests” exercise key components of attacks, subject to some explicit or implicit constraints. The performance of the system as a consequence of the application of those tests is the result of the method. Where it is impractical to apply the tests to the system itself, a model of the system may suffice. The functional approach focuses on threats and protections. A threat model, a list of vulnerabilities, and the likelihood of success of the threats against the vulnerabilities are weighed against the assets, protections, and the likelihood of success of the protections against the threats. The comparative approach presents an explicit standard. An owner compares the owner's system and/or procedures with the standard. Note that there is no explicit system model involved here as there is in the temporal approach. Neither is there an explicit list of threats and assets here as there is in the functional approach.

An engagement consists of experts looking for any way, within given bounds, to compromise assets. An exercise links experts and owners together in order to test the protection on assets particular to a given system. Compliance testing is a more formal way of describing "door rattling." The tests included in methods of this type are such that the owner can execute them himself without the aid of an expert. A sequence method type consists of a series of steps, usually posed as questions, and sometimes in a form as complicated as a flowchart. An assistant method type keeps track of combinations of lists such as threats, vulnerabilities, and assets. A matrix method type is a table lookup. A principles method type, like all of the comparative types, is a list. A best practice method type is a list but it is more specific than a principles list. An audit method type is a list but it is more specific than a best practices list.

Scant classification methods existed prior to Campbell and Stamp, 2004. They include a bifurcation scheme into quantitative versus qualitative methods. AS/NZS 4360, 1999, adds a third element to the scheme, making it quantitative vs. semi-quantitative vs. qualitative. Another example classification scheme is von Solms' traditional assessments vs. baseline controls. BS 7799, 1999, is an example of a baseline control. These classifications did not offer much insight into method selection. The paragraphs that follow review some known conceptual risk assessment models.

		Approach		
Level		**Temporal**	**Functional**	**Comparative**
3	Abstract (Expert)	Engagement Red Team (e.g., IDART™)	Sequence AS/NZS 4360 FIPS PUB 191 IAM IEC/ISO TR 13335 Jelen Kaplan & Garrick NIST 800-30 Schneier	Principles CoCo Freudenburg GAISP GAPP OECD
2	Mid-Level (Collaborative)	Exercise Force on Force Penetration Testing	Assistant Manello OCTAVE RAM-W VSAT™	Best Practice DOE's 21 Steps e-Commerce ISF ITIL LfLO NIST 800-53 PoLO
1	Concrete (Owner)	Compliance Testing security scripts (e.g., SATAN, Nessus) "door rattling"	Matrix AMSA CRAMM RiskWatch SSAGT	Audit BS 7799 CobiT® SSAG Trust Services

Table 2 Example Classification
Source : Campbell and Stamp, 2004

Proposed Conceptual Framework

The derivation of a conceptual framework for risk analysis reveals all its dimensions and affords an exhaustive account of threats and assets. Fig. 1 presents an overall schematic of the relationship of **risk** to its ***four dimensions*** (the environment/community, the humans, the management, and the threat) as outlined in this study and as inspired by the works of Quarantelli, 1980, on disaster evacuations. The framework uses two distinct domains: that of the inherent global variables, which describe pre-existing information; and that of the local variables, which provide the basis for how an individual or a group reacts to a specific threat. The global community includes all initial variables of the evacuation—those that are not affected by any kind of pedestrian or management behavior once the evacuation starts. This information is to be taken from chronicled data and from emergency management agencies.

The global domain has two main components: the community and the threat itself. The community encompasses the physical environment, the persons and organizations that evolve within this environment, including its government, and outside entities such as nearby systems that may impact the course of events. The threat component represents the physical effects of the threat and is linked to location, evolution, and physical characteristics.

The community is characterized by a social climate, inherent social links, and numerous assets. The social climate, according to Quarantelli (1980), consists of the social, psychological, political, economic, legal, or historical factors which can affect the evacuation process. Included in this aspect of the model are the demographics of the humans evolving within the community, such as health and financial status.

Various social links, or bonds, tie community individuals to each other. Johnson, Feinberg and Johnston, 1994, document primary, secondary or nested secondary social groups. Primary and secondary groups contain members with primary (spousal, friendship, familial) and secondary ties, respectively. Strong bonds relate primary group members whereas secondary groups constitute more loosely knit social organizations, such as those made up of co-workers or fellow travelers in a tour group. Nested secondary groups embed members holding primary ties with members holding secondary ties and vice versa. For instance, a husband and wife pair forms a nested secondary group together with a vacationing tour group. Included within the global community are the material and conceptual assets/resources available to organizations and individual or groups of humans (Quarantelli, 1980, 1984, Perry, 1994.)

The local domain concerns itself with the actual onset of the threat, the ensuing actual resiliency and actual exposure consequences, the actual and perceived risk, and the end behavior. The global domain bears physically, socially and psychologically on the humans, delineating the local variables, resiliency, exposure, risks and behavior. Whereas the global variables define how a human can potentially react to a threat, it is the local variables that affect real-time or actual behavior.

Material and conceptual assets help enhance the community's preparedness and resilience, or its ability to cope with the threat. It is these available assets that form the basis for the population's vulnerability as the threat unfolds. Hence, the actual resiliency of the evacuees closely relates to the resources that are available through the global domain, including the proximity to evacuation routes. The actual exposure consequences can be interpreted as varying with the intensity of, and proximity to, the threat and the protection that is afforded.

It is the interaction of the actual exposure consequences and the actual resiliency that forms the actual risk inherently posed by the hurricane situation. This variable is a function of the probability of harm and the magnitude of the damage. The actual risk drives the individual (perception) and social (communication, coordination) processes that define the perceived risk. The evacuation behavior ensues from the perceived risk. Drabek's findings suggest that those who develop high levels of perceived personal risk tend to react significantly faster than others (Drabek, 1996).

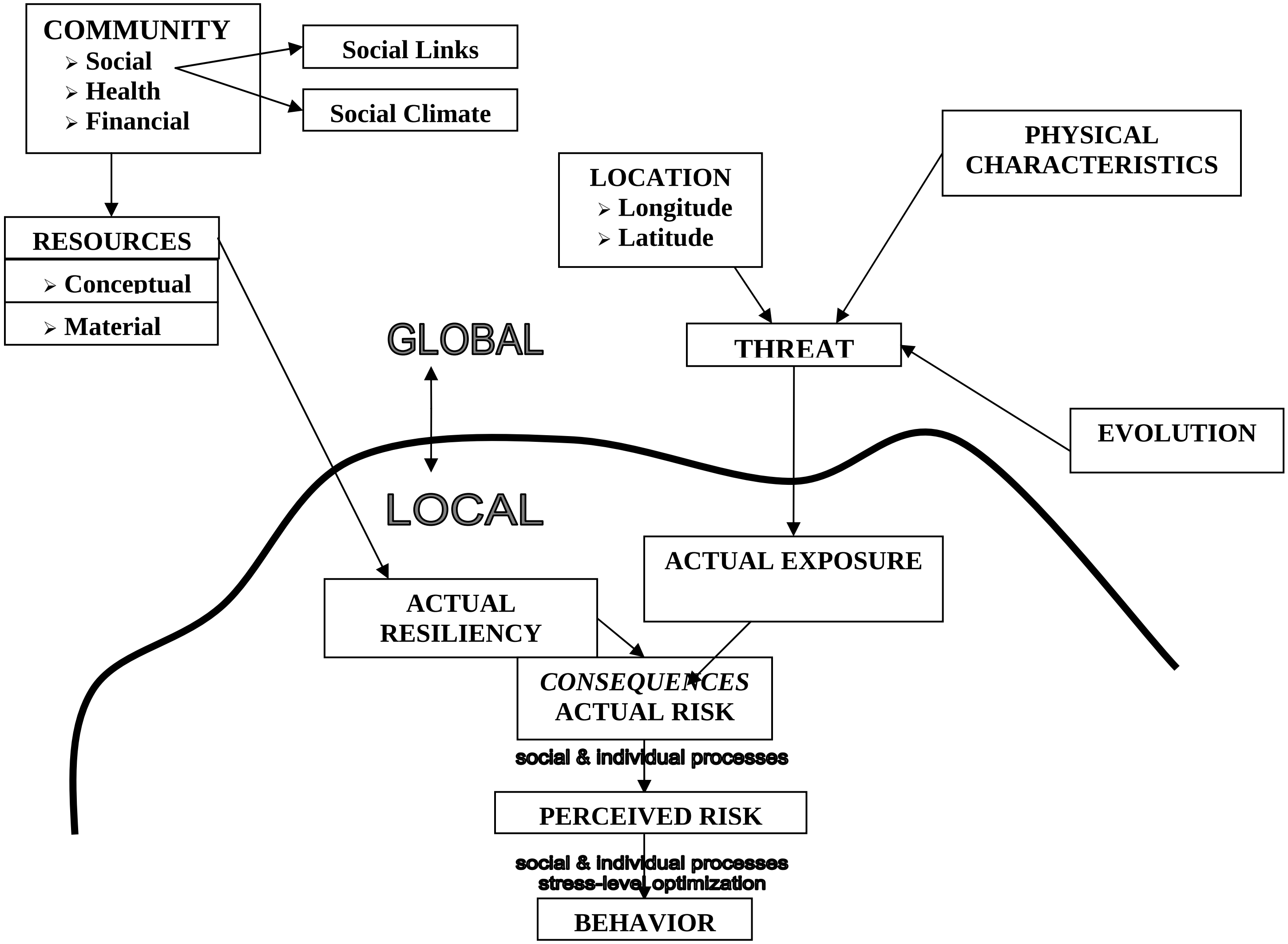
The EPA recommends the following conceptual framework for assessing and enhancing system vulnerability against the unwanted outcome of a terrorist or other intentional attack intended to substantially disrupt the ability to provide a safe and reliable supply of drinking water: 1) the characterization of the water system, including its mission and objectives, 2) the identification and prioritization of adverse consequences to avoid, 3) the determination of critical assets that might be subject to malevolent acts that could result in undesired consequences, 4) the assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries, 5) the evaluation of existing countermeasures, 6) the analysis of current risk and development of a prioritized plan for risk reduction. With regards to item 2 above, Sandia Laboratories suggests that water systems, in general, are vulnerable to four broad classes of attacks: chemical contamination, biological contamination, physical disruption, and disruption of the computerized control network known as the SCADA system. Typical undesired events for water supply, treatment, and distribution may include power loss, system control loss, water supply contamination, and distribution loss.

The EPA recommended that a CWS reviews the potential for tempering or damaging its infrastructure in complying with the Bioterrorism Act. Elements of the infrastructure cited include: the pipes and constructed conveyances, the physical barriers, the water collection (pre-treatment and treatment), the storage and distribution facilities, the electronic (computer or other automated systems utilized), the use, storage and handling of various chemicals, the operation and maintenance of such systems.

Historically, the National Response Center (NRC), in *1983*, specified the major steps of risk assessment as the following: 1) hazard identification, 2) dose response, 3) exposure assessment, 4) risk characterization and 5) risk management. Later work by NRC, 1994, emphasized the iterative nature of incident management, and 1996, the importance of involving the stakeholders in mitigation policies.

Ezell quantifies the vulnerability, defined as a measure of system susceptibility to threat scenarios, of a medium clean sized water system using the Infrastructure Vulnerability Assessment Model (I-VAM). I-VAM is a multi-attribute value model, which scores and ranks the vulnerability of individual water system components. The functional decomposition of a clean water system follows research by AWWA (2002), which cites six subsystems and 14 components. The subsystems include: the source, the transmission, the treatment, the storage, the distribution, and the control. The source includes two (2) components (river and well), the transmission three (3) components (pump station, pipelines, valves), the treatment two (2) components (facilities and processes), the storage three (3) components (clearwell, tank, reservoir), the distribution three (3) components (pump station, delivery piping system, service piping system) and the control one (1) component (SCADA). Ezell fails to consider the use, storage and handling of chemicals as requested by the EPA. However, the approach utilized easily lends itself to the incorporation of this factor.

The model uses as attributes: deterrence, detection, delay, and response. Four value functions, established by subject-matter expects, measure the protection afforded by each decision attribute. Deterrence includes all implemented measures that are perceived by adversaries as too difficult to defeat (Garcia, 2001). Detection aims to detect unauthorized actions through sensing, and to inform the control center of the same. Delay is the time during which adversary penetration is impeded (Garcia, 2001). Response is the time necessary to respond to a threat (Garcia, 2001). The weights applied to the attributes, in determining the vulnerability of each component, were also established by subject-matter expects. Moving up the hierarchy from the component level to the subsystem level, or from the subsystem level to the system level, higher level scores are determined by a weighted average of the lower level scores achieved.


COMMUNITY
Social
Health
Financial
Social Links
Social Climate
PHYSICAL CHARACTERISTICS
LOCATION
Longitude
Latitude
RESOURCES
Conceptual
Material
GLOBAL
THREAT
EVOLUTION
LOCAL
ACTUAL EXPOSURE
ACTUAL RESILIENCY
CONSEQUENCES
ACTUAL RISK
social & individual processes
PERCEIVED RISK
social & individual processes
stress-level optimization
BEHAVIOR

Selection of Risk Assessment Methods

The review of the known classification schemes and conceptual frameworks for risk assessment has led to valuable insights into the optimal selection of a method for a given facility. The classification scheme proposed by Campbell and Stamps, 2004, lends itself to a selection scheme. Already, the levels of this classification were assigned by the original authors to specific assessments based on the level of expertise or familiarity of the study conductors. The assignment of the varied approaches remains unsettled.

The imposition of design analysis standards/codes, as done with comparative risk assessments, to ensure safety/security/surety has proven detrimental in fire safety engineering by stifling/limiting design creativity (Meacham, 1996). Hence, the recent move toward performance-based design analyses, which minimize the use of prescriptive design constraints. A similarity can be established between performance-based design analyses and temporal risk assessment. The both entail flexibility in design given that performance criteria are met. Previous observations suggest that temporal studies are best suited for innovative and complex designs, whereas comparative studies are best suited for the more common and mainline designs.

Collection of Risk Assessment Data

According to Sandia Laboratories, literature searches that cover the past 100 years reveal very few malevolent attacks on the water infrastructure in the United States. The information that is available is thus of limited use to predict the types of attacks that might be perpetrated in the coming years. Hence, the need for a conceptual framework that creates an exhaustive list of the potential threats and assets to consider in vulnerability or risk assessments.

According to the National Plan for Research and Development in Support of Critical Infrastructure Protection, 2004, the evaluation of threats and their likelihood is drawn from multiple sources of information and analysis of different types of threats and potential attackers.

Conclusions

This article presents a review of classification schemes and conceptual frameworks for assessing risk or vulnerabilities at water resource and other facilities. Based on the review, it derives guidelines for selecting risk assessment methods. The guidelines build on previous work by Campbell and Stamp, 2004, of Sandia Laboratories. Latter work selected methods based on the level of expertise, in risk assessment, and the level of familiarity, with the facility, of the analyst. This selection scheme was extended to reflect the design flexibility afforded by the methodological approach in assessing risk. Performance-based methods, such as the temporal and functional methods, which tolerate variations in design, are better suited for innovative and complex system designs. Those, such as the comparative methods, which promote rigid design standards, suit best the facilities with commonly encountered designs.

References

Aho, A. V., R. Sethi, J. D. Ullman, “Compilers: Principles, Techniques, and Tools.” Addison-Wesley. Reading, Massachusetts. 1986.

Alberts, C. J. and A. J. Durofee, “An Introduction to the OCTAVESM Method.” http://www.cert.org/octave/methodintro.html.

Alexander, C., S. Ishikawa and M. Silverstein, A Pattern Language: Towns, Buildings, Construction. Oxford University Press. 1977. ISBN 0-19-501919-9.

AMSA, “Asset Based Vulnerability Checklist for Wastewater Utilities ©.” January 2002.

AS/NZS 4360:1999 Risk Management.

BS 7799-1:1999 Information security management—Part 1: Code of practice for information security management. BS 7799-2:1999 Information security management—Part 2: Specification for information security management systems.

Campbell, P. L. and J. E. Stamp, “A classification Scheme for Risk Assessment Methods.” Sandia Laboratories, IORTA Publications, SAND2004-4233, Albuquerque, New Mexico, 2004.

Cazemier, J. A., P. L. Overbeek and L. M. C. Peters, “Best Practice for Security Management.” The ITIL Infrastructure Library. Office of Government Commerce (OCG). 1999. ISBN 0 11330014 X.

Checkland, P., Systems Thinking, Systems Practice. John Wiley & Sons, 1993.

CobiT 3nd Edition: “Control Objectives for Information and Related Technology (CobiT).” 3rd Edition. July 2000. Published by Information Technology Governance Institute (ITGI). ISBN 1-893209-13-X.

CoCo: Criteria of Control Board. The Canadian Institute of Chartered Accountants. “Guidance on Control.” November 1995. ISBN 0-88800-436-1.

CRAMM: UK Government Risk Analysis & Management Method. Insight Consulting. http://www.insight.co.uk/index.htm.

Department of Energy (DOE), “21 Steps to Improve Cyber Security of SCADA Networks.” (citation unknown)

e-Commerce Security – Enterprise Best Practices. Information Systems Audit and Control Foundation (ISACF). ISBN 1-893-209-10-5.

FIPS PUB 191. “Guideline for the Analysis of Local Area Network Security.” November 9, 1994.

Fried, S. D., “Penetration Testing.” Chapter 15 of the Information Security Management Handbook. Fifth Edition. Tipton & Krause, editors. Auerbach Publishers. Boca Raton, Florida. 2004.

Freudenburg, W. R., “Risky thinking: facts, values and blind spots in societal decisions about risks.” Reliability Engineering and System Safety 72 (2001), pp. 125-30.

GAISP: Information Systems Security Association (ISSA), “Generally Accepted Information Security Principles.” GAISP V3.0. www.gaisp.org.

GAPP: Marianne Swanson, Barbara Guttman, “Generally Accepted Principles and Practices for Securing Information Technology Systems.” NIST Special Publication 800-14, September 1996.

Gouldby and Samuels, “Language of Risk: Project Definitions”. FLOODsite Report T34/04/01, http://www.floodsite.net, 2005.

Hamill, J. T., R. F. Deckro, J. M. Kloeber Jr., T.S. Kelso, “Risk Management and the Value of Information in A Defense Computer System.” Military Operations Research, V7 N2 2002, pp. 61-81.

Hare, C., “Firewalls, Ten Percent of the Solution: A Security Architecture Primer.” Chapter 121 of the Information Security Management Handbook. Fifth Edition. Tipton & Krause, editors. Auerbach Publishers. Boca Raton, Florida. 2004.

IAM: “INFORMATION ASSESSMENT METHODOLOGY. INFOSEC ASSESSMENT METHODOLOGY COURSE. INFOSEC ASSESSMENT TRAINING AND RATING PROGRAM.” from www.nsa.gov.

Information Design Assurance Red Team (IDART™) at Sandia National Laboratories. http://www.sandia.gov/idart.

ISF: Information Security Forum, “The Standard of Good Practice for Information Security.” Version 4.0. March 2003.

ISO/IEC TR 13335 Information Technology--Guidelines for the management of IT Security.

Jelen, G. F., “A New Risk Management Paradigm for INFOSEC Assessments and Evaluations.” Computer Security Applications, 11th Annual Conference. 1995. pp. 261-7.

Kaplan, R., “A Matter of Trust.” Chapter 61 of the Information Security Management Handbook. Fifth Edition. Tipton & Krause, editors. Auerbach Publishers. Boca Raton, Florida. 2004.

Kaplan, S. and B. J. Garrick, “On the Quantitative Definition of Risk.” Risk Analysis, Vol. 1, No. 1, 1981, pp. 11-27.

LfLO: GAO/AIMD-98-68 Information Security Management. (US General Accounting Office Accounting and Information Management Division, “Executive Guide. Information Security Management. Learning From Leading Organizations.”) May 1998.

Manello, C. and W. Rocholl, “Security Evaluation: A Methodology for Risk Assessment.” IS Audit and Control Journal. Vol 6, pp. 42-6. 1997.

Meacham, B. J. The evolution of performance-based codes and fire safety design methods, NIST-GCR-98-761, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Muncaster, G. and E. J. Krall, “An enterprise view of defensive information assurance.” Milcom 1999: IEEE Military Communications Conference Proceedings, Atlantic City, NJ, pp. 714-8.

NIST 800-30: Stoneburner, G., A. Goguen and A. Feringa, “Risk Management Guide for Information Technology Systems.” NIST Special Publication 800-30. October 2001.

NIST 800-53: Ross, R., G. Stoneburner, S. Katzke, A. Johnson and M. Swanson, “Recommended Security Controls for Federal Information Systems.” NIST Special Publication 800-53. “Initial Public Draft.” October 2003.

OECD, “OECD Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security.” Paris: OECD. July 2002. www.oecd.org.

Office of the Press Secretary, “Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection”. White House, Washington, D.C., 2003.

PoLO: U.S. General Accounting Office (GAO), “Information Security Risk Assessment: Practices of Leading Organizations.” Exposure Draft. GAO/AIMD-99-139. August 1999.

RAM-W: “Risk Assessment Methodology for Water Utilities,” Second Edition. Awwa Research Foundation. Denver, Colorado. 2001.

RiskWatch, “How to do a Complete Automated Risk Assessment: A Methodology Review.” AWhite Paper available at www.riskwatch.com.

Schneier, B., “Beyond Fear: Thinking Sensibly About Security in an UncertainWorld.” Copernicus Books, New York. 2003. ISBN 0-387-02620-7.

Security, Research and Business, 14-16 May 1997, Copenhagen, Denmark. pp. 91-98.
[43] VSAT™ Users Page: http://www.vsatusers.net/.

Skoudis, E., “Hacker Tools and Techniques.” Chapter 10 of the Information Security Management Handbook. Fifth Edition. Tipton & Krause, editors. Auerbach Publishers. Boca Raton, Florida. 2004.

SSAG: Swanson, M. “Security Self-Assessment Guide for Information Technology Systems.” NIST Special Publication 800-26. November 2001.

SSAGT: Pacific Northwest Laboratories, “Safeguards and Security Survey and Self-Assessment Guide and Toolkit.” (This material is available from PNL on a CD by calling (509) 375-4349.)

Stamp, J., J. Dillinger and W. Young, Sandia Laboratories, IORTA Publications, SAND2003-1772-C, Albuquerque, New Mexico, 2003.

Trust Services: American Institute of Public Certified Accountants (AICPA), Canadian Institute of Chartered Accountants (CICA), “Suitable Trust Services Criteria and Illustrations.” 2003. www.aicpa.org.

Von Solms, R., “Can Security Baselines replace Risk Analysis?” IFIP TC 11 Conference on Information.